MISSOURI DEPARTMENT OF MENTAL HEALTH

Dorn Schuffman, Department Director

DEPARTMENT OPERATING REGULATION NUMBER
DOR 8.330

CHAPTER	SUBCHAPTER	EFFECTIVE DATE	NUMBER OF PAGES	PAGE NUMBER
Regulation Compliance	HIPAA Regulation.	Sept. 1, 2003	4	1

SUBJECT	AUTHORITY	History
Data Security	630.050	See below

PERSON RESPONSIBLE	SUNSET DATE
Director, Office Information Systems	

Purpose: To prescribe practices which secure electronic consumer protected health information in compliance with federal law and best information management practices and in accordance with 45 CFR 164.530 (c) (1) and (2), and 45 CFR Part 2.

Application: Applies to Department of Mental Health, its facilities and workforce.

(1) Contents

- (A) Definitions
- (B) Data Security
- (C) Sanctions
- (D) Review Process
- (E) DOR Control

(2) Definitions

(A) Computer Systems – Computers connected to local and statewide communication networks, database storage or electronic records systems, Internet or email or other DMH computing devices such as PDA's or stand-alone PC's.

(B) DMH Network – Electronic network allowing access to the DMH's personal computers, facility-based systems, and centrally-based systems (e.g mainframe, server, desktop, etc.) and electronic data.

(C) Local Area Network – Electronic network access allowing access to an individual facility's electronic data and computers.

(D) Network attached computer – Any computer with access to a local area network and/or the DMH network.

(E) DMH Workforce – Includes employees, volunteers, contract workers, trainees and other persons who are in a DMH facility or Central Office on a regular course of business. This shall include client workers employed by the DMH or any of its facilities.

(F) Client/Consumer - Consumer, any individual who has received or is receiving services from a Department of Mental Health state operated facility.

(G) Restricted Access – Computer systems with access limited to specific systems, activities, or files.

(H) Chief Security Officer (Chief Security Officer) - Individual designated by the DMH to oversee all activities related to the development, implementation, maintenance of, and adherence to Department and facility policies and procedures covering the electronic and physical security of, and access to, protected health information and other DMH data in compliance with federal and state laws and regulations.

(I) Local Security Officer (LSO) - Individual designated by a facility CEO to oversee facility information and physical security practice and policy compliance and to coordinate those activities with the Chief Security Officer.

(J) Media – Backup tapes, hard drives, floppy diskettes, CDs, zip drives cartridges, optical, and paper hard copies, etc.

(K) Protected Health Information (PHI) – Individually identifiable health information.

(L) CIMOR – Customer Information Management Outcomes and Reporting system.

(3) Data Security

(A) Users shall be automatically logged off their workstations after a maximum period of 15 minutes of inactivity.

(B) The Chief Security Officer may review an audit trail, produced by any Department or facility computer system, of all accesses and changes to client data on a monthly basis and report violations to employee supervisors and other appropriate staff.

(C) Access to DMH networks from public networks shall be protected by access control systems such as firewalls, access control lists, and user authentication under the auspices of designated DMH IT staff.

(D) All databases shall be backed up nightly in their entirety. All other client related data shall be backed up incrementally with a full back up at least once weekly.

(E) The policy of Department of Mental Health is to ensure that no client PHI related data can be recovered or retrieved from any Department of Mental Health owned computer equipment to be surplused or transferred by using the standards maintained on the DMH Standards List.

(F) Access to media containing client data shall be controlled, by designated IT staff through:

1. Access control lists to network media;
2. Physical access control to DMH hardware;
3. Purging DMH data on any type of media before it is surplused or discarded; and
4. Storage of data on media that is backed up.

(G) Designated staff in the Office of Information Systems shall maintain an up-to-date DMH Standards List which prescribes appropriate procedures and practices for data security purposes.

(H) Virus protection for the DMH network shall be maintained by designated IT staff, pursuant to the DMH virus protection procedures listed below.

1. Email Servers. All DMH email servers, including the Central Office bridgehead server, shall be protected using the email-specific anti-virus software listed on the DMH Standards List.
2. Network and Member Servers. All network and member servers shall be protected using the anti-virus software listed on the DMH Standards List.
3. Workstations, laptops, PDAs

a. All workstations, laptops, PDAs or any other device that connects to the DMH network shall be protected using the anti-virus software for that device listed on the DMH Standards List and installed by designated IT staff.

b. Equipment that has not been purchased by DMH shall not be allowed to connect to the DMH network.

4. Virus signature updates

a. Anti-virus server software shall be configured by designated IT staff to check for virus signature updates daily.

b. Anti-virus PC, laptops, PDAs software will check for virus signature updates hourly from the master console of the anti-virus program, as a result of IT staff actions.

c. Special virus signature updates created in the event of a known virus, will be manually pushed by designated IT staff to all servers, PCs, laptops, and PDAs within 24 hours of the time the receipt of the update has been received at the master console.

5. Software Updates

a. Anti-virus software shall be kept by designated IT staff at the current release or no more than one release below the most current release version.

6. Software Support

a. The DMH Director of Information Systems shall maintain a support contract with the anti-virus software vendor(s) to ensure uninterrupted support.

7. Attachments

a. To avoid potentially virus-carrying attachments, designated DMH staff shall not allow certain types of attachments, such as executable and JPEG files to pass through email as defined by the DMH Standards List.

(I) The DMH workforce shall not load software such as games or screensavers, from any source, onto their assigned workstation or any other Department equipment. This software includes but is not limited to software from the internet, a CD, or a floppy diskette. Software shall be loaded on workstations only by designated employees of the Office of Information Systems or facility IT staff.

(J) DMH workstations shall be situated by respective designated IT staff to prevent more than incidental observation of work product.

(4) Sanctions. Failure of workforce members to comply or assure compliance with the DOR may result in disciplinary action, including dismissal.

(5) Review Process. The Chief Security Officer shall collect information from the LSO's during the month of April each year beginning in 2004 for the purpose of providing feedback to the Director, Office of Information Systems and to the Executive Team regarding trends and issues associated with compliance with this regulation. LSO's shall also conduct initial and period reviews of these policies to ensure compliance within their facility.

(6) There shall be no local policies on this topic. The Department Operating Regulation shall control.

History: Original DOR effective January 1, 200. Final DOR effective September 1, 2003.